System Safety after CAIB

NASA Health and Safety Managers Meeting

Mar 2, 2004

Wayne Frazier, Mgr. System Safety
Code QS
Office of Safety and Mission Assurance
NASA Headquarters

"Mission success stands on the foundation of our unwavering commitment to safety"

Administrator Sean O'Keefe January 2003

VITS Discussion Topic

- How are all the studies, review teams, investigation boards, etc. that resulted from the Columbia accident going to affect the S&MA community and NASA?

- What about System Safety?

System Safety after CAIB

- **External drivers**
  - **CAIB Finding 7.1.1 "Throughout its history, NASA has consistently struggled to achieve viable safety programs …..Yet according to multiple high level independent reviews, NASA's safety system has fallen short of the mark." (system??)**
  - **CAIB Finding 7.4-4,"System Safety engineering and management is separated from mainstream engineering, is not vigorous enough to have an impact on system design, and is hidden in the other safety disciplines at NASA Headquarters."**
  - **ASAP, System safety should be organized as in the military services and not part of a quality organization.**

System Safety after CAIB

- **Internal drivers**
  - **Improve the agency wide System Safety Program……. (Direction from J. Lloyd in performance plan for 04)**
  - **Integrate Risk Assessment methodologies into traditional System Safety…. (Direction from Dr.S in 04 mid year performance review)**

System Safety after CAIB

- **Approach**
  - **Try to understand what the CAIB meant.**
    - **"Program managers created huge barriers against dissenting opinion…"**
    - **"Managers demonstrated little concern for mission safety"**
    - **"Imagine the difference if any shuttle manager had said 'Prove to me that Columbia *has not* been harmed'"**
    - **"Shuttle program hazard reporting is seldom used, safety timeouts are at times disregarded, and informal efforts to gain support are squelched"**
    - **"Safety personnel present in the DAT,MER, and MMT were largely silent in the events leading up to loss of Columbia."**
    - **"The Board believes that the safety organization, due to a lack of capability and resources independent of the Shuttle Program was not an effective voice in discussing technical issues or mission operations…"**
  - **(Was the CAIB talking more about a broken risk management decision process vs a fault in the classic system safety design process or agency system safety policy?)**

System Safety after CAIB

- Conduct thorough discussion with Shuttle(and other) program safety managers at HQ and centers to understand development process and solicit suggested improvements to make system safety more vigorous to have a greater "impact on system design"
- Provide more System Safety focus in NPR 7120.5 rewrite to address CAIB's, "separation from mainstream engineering"
- If needed develop a stand alone System Safety policy/procedure
- Expand OEP reviews to add more emphasis to system safety processes/assessments/risk communication/risk management (This may require changing OEP charter.) (HQ System Safety personnel will attend more OEP)

System Safety after CAIB

- Resurrect SSARMAC (System Safety and Risk Management Assistance (Advisory) Committee to develop better:
  - Level 1 requirements
  - System Safety metrics
  - Methods of risk communication
  - Ways to interface with ITA
  - Skills certification/testing
  - Enhanced traditional System Safety matrix with Risk Quantification (and standardize across agency?)
- Focus Process Verifications (PV) more on system safety (more programmatic approach and policy implementation vs only policy)
- Consider ways of applying AOA's to programs (SS aspect)
- Enhance System Safety emphasis/topics at Safety directors mtgs

System Safety after CAIB

Any more thoughts?

System Safety after CAIB